Practitioner's Docket No. 770P009665-US(PCT)

CHAPTER II

Preliminary Classification:

Proposed Class:

Subclass:

NOTE: *"All applicants are requested to include a preliminary classification on newly filed patent applications. The preliminary classification, preferably class and subclass designations, should be identified in the upper right-hand corner of the letter of transmittal accompanying the application papers, for example 'Proposed Class 2, subclass 129.'" M.P.E.P., § 601, 7th ed.*

TRANSMITTAL LETTER TO THE UNITED STATES ELECTED OFFICE (EO/US)

(ENTRY INTO U.S. NATIONAL PHASE UNDER CHAPTER II)

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US99/05891	18 March 1999	18 March 1998

TITLE OF INVENTION

TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE

APPLICANT(S)

Edward J. NACLERIO

Box PCT
Assistant Commissioner for Patents
Washington D.C. 20231

ATTENTION: EO/US

CERTIFICATION UNDER 37 C.F.R. § 1.10*
(Express Mail label number is mandatory.)
(Express Mail certification is optional.)

I hereby certify that this Transmittal Letter and the papers indicated as being transmitted therewith is being deposited with the United States Postal Service on this date 18 September 2000, in an envelope as "Express Mail Post Office to Addressee" Mailing Label Number EL627420453US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Deborah J. Clark

(type or print name of person mailing paper)

Deborah J. Clark

Signature of person mailing paper

WARNING: *Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. § 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.*

"WARNING: *Each paper or fee filed by "Express Mail" **must** have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. § 1.10(b).*
*"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will **not** be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.*

NOTE: To avoid abandonment of the application, the applicant shall furnish to the USPTO, not later than 20 months from the priority date: (1) a copy of the international application, unless it has been previously communicated by the International Bureau or unless it was originally filed in the USPTO; and (2) the basic national fee (see 37 C.F.R. § 1.492(a)). The 30-month time limit may not be extended. 37 C.F.R. § 1.495.

***WARNING:** Where the items are those which can be submitted to complete the entry of the international application into the national phase are subsequent to 30 months from the priority date the application is still considered to be in the international state and if mailing procedures are utilized to obtain a date the express mail procedure of 37 C.F.R. § 1.10 must be used (since international application papers are not covered by an ordinary certificate of mailing—See 37 C.F.R. § 1.8.*

NOTE: Documents and fees must be clearly identified as a submission to enter the national state under 35 U.S.C. § 371 otherwise the submission will be considered as being made under 35 U.S.C. § 111. 37 C.F.R. § 1.494(f).

I. Applicant herewith submits to the United States Elected Office (EO/US) the following items under 35 U.S.C. § 371:

a. ☒ This express request to immediately begin national examination procedures (35 U.S.C. § 371(f)).

b. ☒ The U.S. National Fee (35 U.S.C. § 371(c)(1)) and other fees (37 C.F.R. § 1.492) as indicated below:

2. Fees

CLAIMS FEE	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
☐*	TOTAL CLAIMS 3	3 −20=	0	× $18.00=	$ 0
	INDEPENDENT CLAIMS 3	3 −3=	0	× $78.00=	0
	MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $260.00	
BASIC FEE**	☒ U.S. PTO WAS INTERNATIONAL PRELIMINARY EXAMINATION AUTHORITY Where an International preliminary examination fee as set forth in § 1.482 has been paid on the international application to the U.S. PTO: ☒ and the international preliminary examination report states that the criteria of novelty, inventive step (non-obviousness) and industrial activity, as defined in PCT Article 33(1) to (4) have been satisfied for all the claims presented in the application entering the national stage (37 C.F.R. § 1.492(a)(4)) ..... $96.00 ☐ and the above requirements are not met (37 C.F.R. § 1.492(a)(1)) ..... $670.00 ☐ U.S. PTO WAS NOT INTERNATIONAL PRELIMINARY EXAMINATION AUTHORITY Where no international preliminary examination fee as set forth in § 1.482 has been paid to the U.S. PTO, and payment of an international search fee as set forth in § 1.445(a)(2) to the U.S. PTO: ☐ has been paid (37 C.F.R. § 1.492(a)(2)) ..... $690.00 ☐ has not been paid (37 C.F.R. § 1.492(a)(3)) ..... $970.00 ☐ where a search report on the international application has been prepared by the European Patent Office or the Japanese Patent Office (37 C.F.R. § 1.492(a)(5)) $840.00				96.00
	Total of above Calculations				= 96.00
SMALL ENTITY	Reduction by 1/2 for filing by small entity, if applicable. Affidavit must be filed also. (note 37 C.F.R. § 1.9, 1.27, 1.28)				–
	Subtotal				
	Total National Fee				$ 96.00
	Fee for recording the enclosed assignment document $40.00 (37 C.F.R. § 1.21(h)). (See Item 13 below). See attached "ASSIGNMENT COVER SHEET".				
TOTAL	Total Fees enclosed				$ 96.00

*See attached Preliminary Amendment Reducing the Number of Claims.

i. ☒ A check in the amount of $96.00 to cover the above fees is enclosed.

ii. ☐ Please charge Account No. _____ in the amount of $ _____. A duplicate copy of this sheet is enclosed.

***WARNING:** *"To avoid abandonment of the application the applicant shall furnish to the United States Patent and Trademark Office not later than the expiration of 30 months from the priority date: * * * (2) the basic national fee (see § 1.492(a)). The 30-month time limit may not be extended." 37 C.F.R. § 1.495(b).*

WARNING: *If the translation of the international application and/or the oath or declaration have not been submitted by the applicant within thirty (30) months from the priority date, such requirements may be met within a time period set by the Office. 37 C.F.R. § 1.495(b)(2). The payment of the surcharge set forth in § 1.492(e) is required as a condition for accepting the oath or declaration later than thirty (30) months after the priority date. The payment of the processing fee set forth in § 1.492(f) is required for acceptance of an English translation later than thirty (30) months after the priority date. Failure to comply with these requirements will result in abandonment of the application. The provisions of § 1.136 apply to the period which is set. Notice of Jan. 3, 1993, 1147 O.G. 29 to 40.*

3. ☒ A copy of the International application as filed (35 U.S.C. § 371(c)(2)):

NOTE: Section 1.495 (b) was amended to require that the basic national fee and a copy of the international application must be filed with the Office by 30 months from the priority date to avoid abandonment. "The International Bureau normally provides the copy of the international application to the Office in accordance with PCT Article 20. At the same time, the International Bureau notifies applicant of the communication to the Office. In accordance with PCT Rule 47.1, that notice shall be accepted by all designated offices as conclusive evidence that the communication has duly taken place. Thus, if the applicant desires to enter the national stage, the applicant normally need only check to be sure the notice from the International Bureau has been received and then pay the basic national fee by 30 months from the priority date." Notice of Jan. 7, 1993, 1147 O.G. 29 to 40, at 35-36. See item 14c below.

a. ☐ is transmitted herewith.

b. ☐ is not required, as the application was filed with the United States Receiving Office.

c. ☒ has been transmitted

i. ☒ by the International Bureau.
Date of mailing of the application (from form PCT/1B/308): 23 September 1999

ii. ☐ by applicant on _____.
Date

4. ☒ A translation of the International application into the English language (35 U.S.C. § 371(c)(2)):

a. ☐ is transmitted herewith.

b. ☒ is not required as the application was filed in English.

c. ☐ was previously transmitted by applicant on _____.
Date

d. ☐ will follow.

5. [X] Amendments to the claims of the International application under PCT Article 19 (35 U.S.C. § 371(c)(3)):

NOTE: The Notice of January 7, 1993 points out that 37 C.F.R. § 1.495(a) was amended to clarify the existing and continuing practice that PCT Article 19 amendments must be submitted by 30 months from the priority date and this deadline may not be extended. The Notice further advises that: "The failure to do so will not result in loss of the subject matter of the PCT Article 19 amendments. Applicant may submit that subject matter in a preliminary amendment filed under section 1.121. In many cases, filing an amendment under section 1.121 is preferable since grammatical or idiomatic errors may be corrected." 1147 O.G. 29-40, at 36.

a. [ ] are transmitted herewith.

b. [ ] have been transmitted

i. [ ] by the International Bureau.
Date of mailing of the amendment (from form PCT/1B/308): _____.

ii. [ ] by applicant on (date) _____.
Date

c. [XX] have not been transmitted as

i. [XX] applicant chose not to make amendments under PCT Article 19.
Date of mailing of Search Report (from form PCT/ISA/210.): 5/28/99.

ii. [ ] the time limit for the submission of amendments has not yet expired. The amendments or a statement that amendments have not been made will be transmitted before the expiration of the time limit under PCT Rule 46.1.

6. [XX] A translation of the amendments to the claims under PCT Article 19 (38 U.S.C. § 371(c)(3)):

a. [ ] is transmitted herewith.

b. [ ] is not required as the amendments were made in the English language.

c. [X] has not been transmitted for reasons indicated at point 5(c) above.

7. [XX] A copy of the international examination report (PCT/IPEA/409)

[X] is transmitted herewith.

[X] is not required as the application was filed with the United States Receiving Office.

8. [X] Annex(es) to the international preliminary examination report

a. [X] is/are transmitted herewith.

b. [X] is/are not required as the application was filed with the United States Receiving Office.

9. [X] A translation of the annexes to the international preliminary examination report

a. [ ] is transmitted herewith.

b. [X] is not required as the annexes are in the English language.

10. ☒ An oath or declaration of the inventor (35 U.S.C. § 371(c)(4)) complying with 35 U.S.C. § 115

    a. ☐ was previously submitted by applicant on _____. Date

    b. ☐ is submitted herewith, and such oath or declaration

        i. ☐ is attached to the application.

        ii. ☐ identifies the application and any amendments under PCT Article 19 that were transmitted as stated in points 3(b) or 3(c) and 5(b); and states that they were reviewed by the inventor as required by 37 C.F.R. § 1.70.

        iii. ☒ will follow.

II. Other document(s) or information included:

11. ☒ An International Search Report (PCT/ISA/210) or Declaration under PCT Article 17(2)(a):

    a. ☒ is transmitted herewith.

    b. ☒ has been transmitted by the International Bureau. Date of mailing (from form PCT/IB/308): 9/23/1999.

    c. ☐ is not required, as the application was searched by the United States International Searching Authority.

    d. ☐ will be transmitted promptly upon request.

    e. ☐ has been submitted by applicant on _____. Date

12. ☒ An Information Disclosure Statement under 37 C.F.R. §§ 1.97 and 1.98:

    a. ☒ is transmitted herewith.

        Also transmitted herewith is/are:

        ☒ Form PTO-1449 (PTO/SB/08A and 08B).

        ☒ Copies of citations listed.

    b. ☐ will be transmitted within THREE MONTHS of the date of submission of requirements under 35 U.S.C. § 371(c).

    c. ☐ was previously submitted by applicant on _____. Date

13. ☐ An assignment document is transmitted herewith for recording.

    A separate ☐ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.

_____

_____

_____

14. ☒ Additional documents:

a. ☒ Copy of request (PCT/RO/101)

b. ☒ International Publication No. WO 99/48055

i. ☒ Specification, claims and drawing

ii. ☐ Front page only

c. ☐ Preliminary amendment (37 C.F.R. § 1.121)

d. ☒ Other

PCT/IB/308; PCT/IB/332; PCT/IB/304; PCT/IPEA/409; PCT/ISA/220; PCT/ISA/210; Demand; PCT/IPEA/408; Response to Written Opinion; PCT/IPEA/402

15. ☒ The above checked items are being transmitted

a. ☒ before 30 months from any claimed priority date.

b. ☐ after 30 months.

16. ☐ Certain requirements under 35 U.S.C. § 371 were previously submitted by the applicant on _____, namely:

AUTHORIZATION TO CHARGE ADDITIONAL FEES

WARNING: *Accurately count claims, especially multiple dependant claims, to avoid unexpected high charges if extra claims are authorized.*

NOTE: "A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.136(a)(3).

NOTE: "Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts; amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account." 37 C.F.R. § 1.26(a).

☒ The Commissioner is hereby authorized to charge the following additional fees that may be required by this paper and during the entire pendency of this application to Account No. **16-1350**.

☒ 37 C.F.R. § 1.492(a)(1), (2), (3), and (4) (filing fees)

WARNING: *Because failure to pay the national fee within 30 months without extension (37 C.F.R. § 1.495(b)(2)) results in abandonment of the application, it would be best to always check the above box.*

☒ 37 C.F.R. § 1.492(b), (c) and (d) (presentation of extra claims)

NOTE: Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 C.F.R. § 1.492(d)), it might be best not to authorize the PTO to charge additional claim fees, except possible when dealing with amendments after final action.

☒ 37 C.F.R. § 1.17 (application processing fees)

☐ 37 C.F.R. § 1.17(a)(1)–(5) (extension fees pursuant to § 1.136(a).

☐ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 C.F.R. § 1.311(b).

NOTE: 37 C.F.R. § 1.28(b) requires "Notification of any change in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying . . . issue fee." From the wording of 37 C.F.R. § 1.28(b): (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.

☒ 37 C.F.R. § 1.492(e) and (f) (surcharge fees for filing the declaration and/or filing an English translation of an International Application later than 30 months after the priority date).

PLEASE SEND ALL CORRESPONDENCE TO:

Reg. No.: 24,622

Tel. No.: (203) 259-1800

Customer No.: 2512

SIGNATURE OF PRACTITIONER

Clarence A. Green

(type or print name of practitioner)

PERMAN & GREEN, LLP

P.O. Address

425 Post Road, Fairfield, Connecticut 06430, USA

PLEASE SEND ALL CORRESPONDENCE TO:

Clarence A. Green
PERMAN & GREEN, LLP
425 Post Road, Fairfield, Connecticut 06430, USA

TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE

The invention relates generally to postage meters (franking machines), and relates particularly to systems in which postage value is stored in a postal security device (PSD) so as to be protected against undetected tampering. The application claims priority from US application no. 60/078,489, filed March 18, 1998, which application is incorporated herein by reference to the extent permitted by the designated and elected States hereto.

Background

In recent years it has been proposed to print postal indicia by means of conventional nonsecure printers such as laser printers, ink-jet printers, and thermal transfer printers. Such printers are termed "nonsecure" because the printer itself is not in a secure housing and because the communications channel linking the printer to other apparatus is nonsecure. Under such a proposal, the question naturally arises what would prevent a user from printing the same postal indicium repeatedly, thereby printing postal indicia for which no money has been paid to the post office. The proposed anti-fraud measure is to store information within the indicia which would permit detecting fraud. The indicium would include not only human-readable text such as a date and a postage amount, but would also include machine-readable information, for example by means of a two-dimensional bar code. The machine-readable information would be cryptographically signed, and would include within it some information intended to make fraud more difficult. The information would typically include an identification of the postage meter license (granted by the meter manufacturer or by the postal authorities, depending on the country), an indication of the number of mail pieces franked, the postage amount, a postal security device identifier about which more will be said later, the date and time, and a zip code or post code of the mail piece addressee.

The typical apparatus for printing such "encrypted indicia" postage includes what is called a postal security device or PSD. The PSD has a secure housing, and within the secure housing are the accounting registers as well as a cryptographic engine. The engine permits cryptographic authentication and signing for communication with an external device such as

the computer of the meter manufacturer or of the post office. The engine also permits creation of postal indicia which contain specified information and which are cryptographically signed. The PSD may well be physically small as compared to traditional postage meters. The PSD may be the size of a PCMCIA card or the size of a smart card.

Within the PSD the memory must be protected against inadvertent damage due to malfunction of the processor of the PSD, for example as set forth in US Pat. No. 5668973, *Protection system for critical memory information* owned by the same assignee as the assignee of the present application. The PSD must handle power failure in a graceful fashion, for example as set forth in US Pat. No. 5712542, *Postage meter with improved handling of power failure*, also owned by the same assignee as the assignee of the present application.

To reduce smudging, the printer may preferably be that described in PCT publication no. 97-46389, *Printing apparatus*, also owned by the same assignee as the assignee of the present application. While it has been proposed that the PSD contain a real-time clock which is keeping time continuously, desirably this requirement may be avoided as described in PCT publication no. 98-08325, *Printing postage with cryptographic clocking security*, also owned by the same assignee as the assignee of the present application. PSDs can form part of a network with multiple printers as described in PCT publication no. 98-13790, *Proof of postage digital franking*, also owned by the same assignee as the assignee of the present application.

The postal authorities face the question how the PSD can be protected from tampering. For example, the entire system of PSDs depends on the use of cryptographic keys. The keys are used for authenticating communications between the PSD and the manufacturer's system or the postal authority's system. Such communications are used to set up and maintain the PSDs, and are used to refill or "reset" the PSDs to reflect the ability to print more postage. The keys are also used to cryptographically "sign" information printed in the postal indicia. If the cryptographic keys were compromised, a user might be able to defraud the post office or the PSD manufacturer or both.

Many approaches have been proposed for protection of such cryptographic keys from compromise. The usual approach is to place the cryptographic keys in a RAM (random access memory) of a type which keeps its contents only so long as the RAM receives power from a battery. The secure housing of the PSD is designed to include a tamper switch, so that if the secure housing is tampered with, the switch opens. The switch interrupts power to the RAM (and, in particular, interrupts battery power to the RAM) and its contents are lost. In this way the information in the RAM (for example, the cryptographic keys) is protected from tampering. Another proposed approach is to employ commercial memory chips (such as the Dallas Semiconductor DS1283 and Benchmarq bq3283) offer a pin on the package which will clear the memory based on a predetermined input voltage level. The tamper switch is set up to apply the predetermined voltage upon detection of tampering.

Many approaches have also been proposed for detection of the tampering. In EP 820 041, for example, it is suggested that the secure housing of an old-style mechanical or electromechanical postage meter be set up to contain an air pressure that is distinctively higher than or lower than normal atmospheric pressure. If the secure housing is violated, the pressure within the secure housing changes to match the ambient pressure. A sensor within the housing detects the pressure change and thus the violation. The sensor disables further function of the postage meter.

The approach of cutting power to a volatile memory such as the RAM discussed above has a drawback in that during periods of power-down, the RAM depends on an internal battery to avoid loss of the information in the RAM. Depending on the requirements of the postal authority, and on design decisions made by the PSD manufacturer, the quantity of data requiring protection may be quite large. The data to be protected may include cryptographic keys used for PSD configuration, keys used for remote resetting (refilling), keys used for signing postal indicia, and keys used for the management of the other keys. In addition it may be desired to protect the bit-images used to generate the human-readable portion of the printed indicia. A RAM big enough to hold all of these important items of data will also draw a non-negligible current from the internal battery. This may lead to a limited and commercially unacceptable battery life.

It would thus be desirable to have a PSD design which protects the many important items of data stored within, and yet which does not draw very much battery power and so permits a commercially acceptable battery life.

Summary of the invention

In accordance with the invention, a postal security device (PSD) contains a nonvolatile memory which does not depend on battery power, such as an EEPROM, and contains a nonvolatile memory which does depend on battery power, such as a static RAM. The PSD also contains an encryption engine. An encryption key is developed and is stored in the static RAM, which is sized to be only large enough to contain the encryption key. A large body of data, too large to fit in the static RAM, is encrypted by means of the encryption engine and with reference to the encryption key, and is stored in the EEPROM. This body of data typically includes cryptographic keys and sensitive bit-images. When the PSD is powered, a large RAM (typically a dynamic RAM) is available to receive the large body of data, decrypted using the encryption key. A tamper switch cuts power to both RAMs in the event of tampering. In this way, the battery power required to maintain the PSD during power-off periods is minimal, and yet the large body of data will be inaccessible in the event of tampering.

Description of the drawing

The invention will be described with respect to a drawing, of which:

Fig. 1 is a schematic functional block diagram of a system according to the invention.

Detailed description

Fig. 1 shows a postal security device (PSD) in accordance with the invention. The PSD has a microprocessor 12 which communicates on a bus 22 with an input/output (I/O) device 18, a memory which does not require battery backup 13 which may be for example an EEPROM or

flash memory, a relatively small RAM 14, a ROM 22, and a larger RAM 16. The I/O device 18 communicates with external apparatus by means of communications channel 19 which may be a serial asynchronous data line. External power 21 and ground 20 are also defined. The larger RAM 16, and most of the other active components, receive external power. The smaller RAM 14 is additionally able to receive power from a backup battery 15, preferably a lithium cell with a very long (e.g. ten year) life. A tamper switch 17 is provided which, when triggered, can cut power to both the small RAM 14 and the large RAM 16.

A large body of data is assumed to require protection from a tampering user. The EEPROM is selected to be large enough to hold this body of data after it has been encrypted. When power is applied and the system is stable, the body of data (or selected portions thereof) is decrypted and transferred to RAM 16. This decryption is performed by the microprocessor 12 executing a decryption routine stored in the ROM 22, and the decryption is done with respect to a decryption key in the RAM 14. Alternatively the decryption may be performed by an optional engine omitted for clarity in Fig. 1. The decrypted data in RAM 16 are used as needed for the ordinary functions of the PSD, which include communicating via the communications channel 19 with a user computer, with a manufacturer's system, or with a postal authority system, and can include generating postal indicia which are to be printed by means of a printer.

When external power 21 is cut off, or when the PSD undergoes a normal power-down routine, the information in the RAM 16 is lost. In contrast, the information in the RAM 14 is preserved even when external power 21 is lost, because of battery 15.

During normal operation the body of data that requires protection from a tampering user (or some portion of it) may be located "in the clear", that is, unencrypted, in the RAM 16. In the event that this data has changed, it may be necessary to encrypt the data and to store it again in the memory 13. This encryption is performed by the processor 12 executing encryption software in the ROM 22, or may optionally be performed by an encryption engine omitted for clarity in Fig. 1.

The power-down condition for the PSD 10 assumes that no power is present at line 21. In that event, the only powered device is RAM 14. RAM 14 was purposefully selected to be large enough to hold the encryption key but not much larger, and in any event is smaller than the large body of data that is understood to require protection from a tampering user. Because of the limited size of the RAM 14, it does not draw as much current from the battery 15 as would be drawn by a larger RAM such as RAM 16. Thus, the battery life is optimized, especially as compared with the shorter battery life that would result if the large body of data were all in battery-backed-up RAM.

Tampering may happen during a time when external power 21 is present. At a minimum, the tamper switch should cut power to the RAM 14. (Or, alternatively, the tamper switch should apply to RAM 14 the predetermined voltage that clears the RAM.) Preferably the tamper switch will also cut power to the RAM 16 (or clear the RAM 16), for the reason that some of the body of sensitive data may be present "in the clear" in the RAM 16, and should not fall into the hands of the tampering user. Alternatively the tamper switch might trigger an interrupt in the processor 12 which would cause the processor 12 to clear the sensitive portions of the RAM 16.

Tampering may also happen during a time when external power 21 is absent. In such a case, the RAM 16 is already, by definition, empty, as it is unpowered. The tamper switch causes the RAM 14 to be cleared. If the tampering user extracts the contents of the memory 13, this is of little significance, because the contents are useless unless decrypted with the assistance of the key that is no longer present in the RAM 14. If the PSD 10 is powered up again after the tampering, the decryption routine will not work because the key of RAM 14 is gone. In addition, desirably the processor 12, under program control, will note the fact that RAM 14 is empty and will immediately attempt to send a message via communications channel 19 to the manufacturer or to the postal authority.

Those skilled in the art will readily appreciate that design considerations may prompt the use of electrical components in addition to or instead of those shown in Fig. 1, none of which depart in any way from the invention. For example, dedicated cryptographic chips may be

employed which take some of the computational burden from the microprocessor. As another example, the particular way in which the tamper switch cuts power to the RAM may be varied, and the particular type of tamper switch may be selected among several types, all without departing in any way from the invention. Those skilled in the art will indeed have no difficulty devising obvious variations and improvements to the invention, all of which are intended to be encompassed by the claims that follow.

Claims

1. A postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type requiring electrical power to maintain the contents thereof, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine, said body of data encrypted by the cryptographic engine with respect to the encryption key.

2. A method for use with a postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type that requires electric power to maintain its contents, said postal security device also comprising a battery powering the second memory and a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory is disconnected from the battery, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, removing power from the second memory.

3. A method for use with a postal security device comprising a secure housing, and within the secure housing a body of data having a size, said postal security device also having within the secure housing means for generating print data for printing of postage indicia, said generating of said print data relying in part on the body of data, said postal security device also having within the secure housing a first memory sized to accommodate the body of data, said first memory of a type not requiring electrical power to maintain the contents thereof, said postal security device also having within the secure housing a second memory not large enough to accommodate the body of data, said second memory of a type that clears its contents upon a predetermined electrical condition, said postal security device also comprising a tamper switch mechanically coupled with the secure housing so that upon tampering with the secure housing the second memory has said predetermined electrical condition, said postal security device further comprising an encryption key stored within said second memory, said postal security device further comprising a cryptographic engine; the method comprising the steps of:

storing the encryption key within the second memory;

encrypting the body of data by the cryptographic engine with respect to the encryption key;

storing the encrypted body of data in the first memory; and

in the event of tampering, causing said predetermined electrical condition.

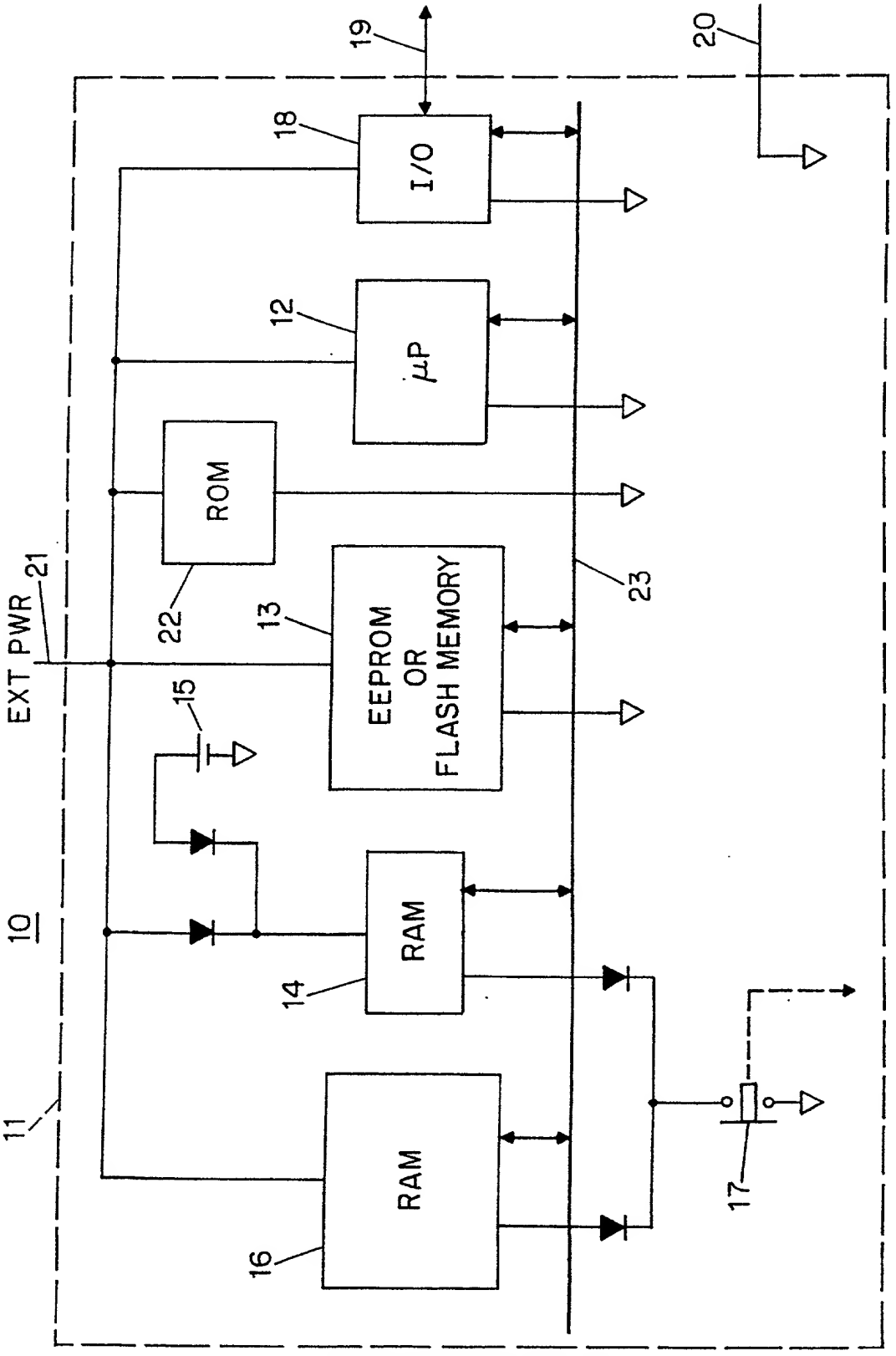
19
20
18
I/O
12
μP
ROM
22
21
EXT PWR
13
EEPROM
OR
FLASH MEMORY
23
15
10
RAM
14
11
RAM
16
17

FIG. 1

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL, CONTINUATION, OR C-I-P)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is of the following type:

(check one applicable item below)

- ☐ original.
- ☐ design.
- ☐ supplemental.

NOTE: If the declaration is for an International Application being filed as a divisional, continuation or continuation-in-part application, do not check next item; check appropriate one of last three items.

- ☒ national stage of PCT.

NOTE: If one of the following 3 items apply, then complete and also attach ADDED PAGES FOR DIVISIONAL, CONTINUATION OR C-I-P.

NOTE: See 37 C.F.R. § 1.63(d) (continued prosecution application) for use of a prior nonprovisional application declaration in the continuation or divisional application being filed on behalf of the same or fewer of the inventors named in the prior application.

- ☐ divisional.
- ☐ continuation.

NOTE: Where an application discloses and claims subject matter not disclosed in the prior application, or a continuation or divisional application names an inventor not named in the prior application, a continuation-in-part application must be filed under 37 C.F.R. § 1.53(b) (application filing requirements — nonprovisional application).

- ☐ continuation-in-part (C-I-P).

INVENTORSHIP IDENTIFICATION

WARNING: If the inventors are each not the inventors of all the claims, an explanation of the facts, including the ownership of all the claims at the time the last claimed invention was made, should be submitted.

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am the original, first and sole inventor *(if only one name is listed below)* or an original, first and joint inventor *(if plural names are listed below)* of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE

SPECIFICATION IDENTIFICATION

the specification of which:

(complete (a), (b), or (c))

(a) ☐ is attached hereto.

NOTE: *"The following combinations of information supplied in an oath or declaration filed on the application filing date with a specification are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 CFR 1.63:*

"(1) name of inventor(s), and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration on filing;

"(2) name of inventor(s), and attorney docket number which was on the specification as filed; or

"(3) name of inventor(s), and title which was on the specification as filed."

Notice of July 13, 1995 (1177 O.G. 60).

(b) ☐ was filed on ____________________, as ☒ Serial No. 09 / 646,489
or ☐ ____________________
and was amended on ________________ *(if applicable).*

NOTE: *Amendments filed after the original papers are deposited with the PTO that contain new matter are not accorded a filing date by being referred to in the declaration. Accordingly, the amendments involved are those filed with the application papers or, in the case of a supplemental declaration, are those amendments claiming matter not encompassed in the original statement of invention or claims. See 37 CFR 1.67.*

NOTE: *"The following combinations of information supplied in an oath or declaration filed after the filing date are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 CFR 1.63:*

"(1) name of inventor(s), and application number (consisting of the series code and the serial number; e.g.,08/123,456);

"(2) name of inventor(s), serial number and filing date;

"(3) name of inventor(s) and attorney docket number which was on the specification as filed;

"(4) name of inventor(s), title which was on the specification as filed and filing date;

"(5) name of inventor(s), title which was on the specification as filed and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration; or

"(6) name of inventor(s), title which was on the specification as filed and accompanied by a cover letter accurately identifying the application for which it was intended by either the application number (consisting of the series code and the serial number; e.g.,08/123,456), or serial number and filing date. Absent any statement(s) to the contrary, it will be presumed that the application filed in the PTO is the application which the inventor(s) executed by signing the oath or declaration."

Notice of July 13, 1995 (1177 O.G. 60).

(c) ☒ was described and claimed in PCT International Application No. PCT/US99/05891, filed on 18 March 1999 and as amended under PCT Article 19 on ____________________ *(if any).*

SUPPLEMENTAL DECLARATION (37 C.F.R. § 1.67(b))

(complete the following where a supplemental declaration is being submitted)

☐ I hereby declare that the subject matter of the

☐ attached amendment

☐ amendment filed on ____________________

was part of my/our invention and was invented before the filing date of the original application, above-identified, for such invention.

ACKNOWLEDGEMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, § 1.56,

(also check the following items, if desired)

☒ and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent, and

☐ in compliance with this duty, there is attached an information disclosure statement, in accordance with 37 CFR 1.98.

PRIORITY CLAIM (35 U.S.C. §§ 119(a)–(d))

NOTE: "The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63. The claim for priority and the certified copy of the foreign application specified in 35 U.S.C. 119(b) must be filed in the case of an interference (§ 1.630), when necessary to overcome the date of a reference relied upon by the examiner, when specifically required by the examiner, and in all other situations, before the patent is granted. If the claim for priority or the certified copy of the foreign application is filed after the date the issue fee is paid, it must be accompanied by a petition requesting entry and by the fee set forth in § 1.17(i). If the certified copy is not in the English language, a translation need not be filed except in the case of interference; or when necessary to overcome the date of a reference relied upon by the examiner; or when specifically required by the examiner, in which event an English language translation must be filed together with a statement that the translation of the certified copy is accurate." 37 C.F.R. § 1.55(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119(a)–(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

(complete (d) or (e))

(d) ☐ no such applications have been filed.

(e) ☐ such applications have been filed as follows.

NOTE: Where item (c) is entered above and the International Application which designated the U.S. itself claimed priority check item (e), enter the details below and make the priority claim.

PRIOR FOREIGN/PCT APPLICATION(S) FILED WITHIN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119(a)-(d)

COUNTRY (OR INDICATE IF PCT)	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 USC 119
			☐ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐
			☐ YES NO ☐

CLAIM FOR BENEFIT OF PRIOR U.S. PROVISIONAL APPLICATION(S)

(34 U.S.C. § 119(e))

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

PROVISIONAL APPLICATION NUMBER	FILING DATE
60 / 078,489	18 March 1998
/	
/	

CLAIM FOR BENEFIT OF EARLIER US/PCT APPLICATION(S) UNDER 35 U.S.C. 120

☐ The claim for the benefit of any such applications are set forth in the attached ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR CONTINUATION-IN PART (C-I-P) APPLICATION.

ALL FOREIGN APPLICATION(S), *IF ANY*, FILED MORE THAN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

PCT/US99/05891 filed 18 March 1999

NOTE: If the application filed more than 12 months from the filing date of this application is a PCT filing forming the basis for this application entering the United States as (1) the national stage, or (2) a continuation, divisional, or continuation-in-part, then also complete ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR C-I-P APPLICATION for benefit of the prior U.S. or PCT application(s) under 35 U.S.C. § 120.

POWER OF ATTORNEY

I hereby appoint the following practitioner(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

(list name and registration number)

Clarence A. Green ~~(24,622)~~
Mark F. Harrington ~~(31,686)~~
Janik Marcovici (42,841)

(check the following item, if applicable)

☐ I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

☐ Attached, as part of this declaration and power of attorney, is the authorization of the above-named practitioner(s) to accept and follow instructions from my representative(s).

SEND CORRESPONDENCE TO

☒ Address

~~Clarence A. Green~~
~~PERMAN & GREEN, LLP~~
~~425 Post Road~~
Fairfield, CT 06430

☐ Customer Number 2512

DIRECT TELEPHONE CALLS TO:
(Name and telephone number)

Clarence A. Green
(203) 259-1800

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

NOTE: Carefully indicate the family (or last) name, as it should appear on the filing receipt and all other documents.

Full name of sole or first inventor

Edward	J.	NACLERIO
(GIVEN NAME)	*(MIDDLE INITIAL OR NAME)*	*FAMILY (OR LAST NAME)*

Inventor's signature Edward J. Naclerio

Date October 24, 2000 Country of Citizenship U.S.A.

Residence 49 Scenic Road, Madison, Connecticut 06443 USA

Post Office Address 49 Scenic Road, Madison, Connecticut 06443 USA

Full name of second joint inventor, if any

(GIVEN NAME)	*(MIDDLE INITIAL OR NAME)*	*FAMILY (OR LAST NAME)*

Inventor's signature ______

Date ______ Country of Citizenship ______

Residence ______

Post Office Address ______

Full name of third joint inventor, if any

(GIVEN NAME)	*(MIDDLE INITIAL OR NAME)*	*FAMILY (OR LAST NAME)*

Inventor's signature ______

Date ______ Country of Citizenship ______

Residence ______

Post Office Address ______

(check proper box(es) for any of the following added page(s) that form a part of this declaration)

☐ **Signature** for fourth and subsequent joint inventors. *Number of pages added* ________

• • •

☐ **Signature** by administrator(trix), executor(trix) or legal representative for deceased or incapacitated inventor. *Number of pages added* ________.

• • •

☐ **Signature** for inventor who refuses to sign or cannot be reached by person authorized under 37 CFR 1.47. *Number of pages added* ________

• • •

☐ Added page for **signature** by one joint inventor on behalf of deceased inventor(s) where legal representative cannot be appointed in time. (37 CFR 1.47)

• • •

☐ Added pages to combined declaration and power of attorney for divisional, continuation, or continuation-in-part (C-I-P) application.

☐ Number of pages added ________

• • •

☐ Authorization of practitioner(s) to accept and follow instructions from representative.

• • •

(if no further pages form a part of this Declaration, then end this Declaration with this page and check the following item)

☒ This declaration ends with this page.